Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1729 08/07/15

~ Mac Users, Don’t Freak! ~ Win 10 for Xbox One! ~ Next WoW Expansion!

-* Bushnell: Why Life Is A Game *-
-* Facebook Rolls Out Security Checkup *-
-* School District Monitors Students, Teachers *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Sorry, as usual, I’m running late again this week - so I’ll keep it short. Did you catch the GOP "debate" the other night? I was working, so I missed it. I hope to see some highlights on the news over the next couple of days. I heard that Donald Trump was his typically outspoken self again! While I don’t know what his chances might be to get nominated, it is refreshing to hear a candidate speak out candidly rather than try to "act" like a politician! I may not agree with all that he has to say, I’ll give him credit for speaking his mind!

What a weird day we had this past Tuesday as far as the weather was concerned. Early in the afternoon, I had one of my dogs outside to do her business. All of the sudden, the sky got very dark; and I started seeing spots appear on the walkway - it was starting to rain a little. Then the rain increased a bit; and then I noticed that the spots were starting to "splatter". And, I was starting to feel something other than raindrops hitting me - it was starting to hail! I got the dog inside just in time, because the skies were flashing bright white, the thunder was raoring, and the skies opened up with rain and dime-sized hail stones! What a racket! The storm lasted about 10-15 minutes, but that was enough. I looked at my yard and all I could see were small lakes everywhere! The sky cleared for awhile, but we got a repeat storm shortly after I got to work. I missed getting soaked by about 5 minutes! We haven’t had a storm like those in my area for quite some time! Fascinating, as long as you didn’t get caught outside in it!

Until next time...

=~=~=~=

Farewell EasyMiNT

EasyMiNT 1.90 Final Version

7/28/15

After much of thinking about it, I have decided to quit the EasyMiNT project, the 1.90 will be the last version. Because my interests are

going in another direction and I’m a little bit tired of programming EasyMiNT I take this step. Furthermore the feedback on the last beta version was very low and it seems rpm isn’t developed anymore and most of the rpm packages are outdated. The freemint community is a little bit chaotic and several guys are working on it but not very good together.

It was not very easy for me to make this decision after about 15 years, but it has to be.

I will not give any support anymore and will not answer questions about EasyMiNT it’s final-take-as-is software. But the website will be still online for now.

So I wish to thank all people who helped me with this project, without them it never were realized.

Have fun!

Playing With The Firebee, continued

In my last submission I was discussing my research into the latest Atari Clones and my experience with using the Raspberry Pi System. This brings me to the one Atari Clone I was researching the whole time but didn t discuss much until now. That would be the FireBee. This is the over decade long Atari ColdFire Project the resulted in the FireBee. http://acp.atari.org/ The site is worth a look at and read. It truly is amazing the amount of time and effort that the group of people went through to dream, design, and produce a machine to sell to the public. What is even more impressive is that as far as I am aware all the people volunteered their time to the project. It is one thing to dream of something that ambitious. Then another to actually follow through but at the end of the day some one has to purchase the machine to pay for all the Research and Development. Maybe not so surprising is that there are enough demand from Atari Computer Enthusiasts out there that are willing to pay for such a machine. Though very small in numbers to the general Windows, Mac, and Unix there are still Atari Computers used for production work. Then there are the folks like myself who prefer running on real hardware instead of emulators. Emulators are great but if a real machine is available and affordable that is my preferred choice.

Medusa Computer Systems is producing and selling the FireBee System. Medusa has a long history with working with Atari TOS Computers as they had produced the T40 and Hades Atari Clone Systems over the years. The specifications on the FireBee can be found here: http://medusacomputer.com/firebee.html You may look at the specs and see 266mhz CPU with 512MB of RAM and think this is nothing compared to the multi core, multi ghz CPUs of a modern computer and more RAM than an Atari Computer Users entire hard drive or floppy collection. Guess what you are right! But compared to an Atari ST, TT, or Falcon this is an amazing leap forward. For the Atari Computer users out there they are aware that Atari programs have very small memory and storage requirements. The system board costs 599 Euros, the cool looking case in multiple colors 79 Euros, and FreeMiNT preinstalled on a 16GB CF Flash Card is 15 Euros.

In Mid 2014 I contacted the Atari Coldfire Project (ACP) about the

availability of a Firebee system. At that time there were none available and that a run was being planned for the end of 2014. In December 2014 I contacted ACP again and was told that the production run did not happen as there were some revisions that were being planed to be done on the system and that they wanted those completed and tested before any new systems were to be produced. I didn t think a whole lot about the FireBee for a long time after that. I started back into working with the Raspberry Pi but still had no luck with networking. Did a little more with Aranym but still didn t get exactly what I was after. Then in May 2015 I contacted ACP again inquiring about the status of a FireBee. I was told the same thing as in December 2014 but if I wanted there a board available that everything worked on it but the PCI bus/slot was defective. Since I would never be adding a video card to the system I agreed to purchase this unit. I sent payment via Paypal and then waited. I was told that assembling, testing and shipping would take about 30 days before I would see the unit.

Well on June 30 the FireBee arrived. I opened the box and looked quickly at the Basic Information Sheet on the FireBee and other paperwork on the unit. Then went off to the basement with the FireBee and put it on the desk that doesn t get used much so I set it up and could leave it there for as long as I wanted. At that desk was already a Mac G5 Tower so I used that USB mouse and keyboard. The monitor there was a HP 15 inch LCD capable of 1024x768 resolution. Also at that desk was an old 10MB Hub for networking. I found a DVI to VGA adapter in my box of parts and hooked everything up and turn it on. After about 30 seconds the Fuji Symbol was on the screen and MiNT started loading. After a few more seconds the First Boot Menu came up and asked which Desktop I wanted to run. Choices are Thing 1.27, Thing 1.29b (German only) and Teradesk. Then I noticed that the mouse and keyboard appeared not to be working. I powered the FireBee off and looked at the connections and they looked good so I went found another keyboard and mouse which also happened to be another Apple Mac keyboard and a Microsoft Mouse. Same thing when I booted the mouse and keyboard appeared to not work. I went and found another set this time a Dell keyboard. Success finally I was at the Desktop choice menu again. Personally I think Thing looks nicer but I chose Teradesk as I have been using it more recently with my Aranym setups and like having the Right Mouse Click as being a double click like Ease Desktop that I had on my TT many years ago. Plus I can always choose Thing at anytime if I want. After the Desktop selection a message comes up and tells you to run the Video Setup program to select the best resolution for your monitor as the initial boot resolution is 640x480. I ran the program and it suggested properly 1024x768 for my monitor. I ran the option to Test the resolution and got a set of horizontal rainbow color bars. I thought something was wrong so I didn t select that resolution and left it at 640x480 for the time being. Since I was now at the Desktop I clicked on the included Web Browser called Netsurf just to see how fast the FireBee was on the Web. I typed in an address to a Web Site and got the message No route to Host . Which basically meant that the FireBee did not get an IP Address from my router. I did notice on the Hub though that there was a lot of activity on the FireBee port and that the Hub had an Error. I shut the FireBee down and checked all connections and switch monitors to a 17 inch CRT monitor. I turned the FireBee back on and ran the Video Setup program and got the same horizontal colored rainbows. I left the video at 640x480 still and also still did not get an IP Address from DHCP from my router. I had seen the Hub exhibit the exact same behavior many years ago while working on at that time a high end server. What the issue was with the server was that the Network Card could only support 100/1000MB and did not go as slow as 10MB. I switched the Hub to a 10/100MB Switch. When I tried

after that the FireBee was able to get an IP Address and I was able to connect to the Web! At this point it was late in the evening so I shut everything down.

I contacted Mathias Wittau over at ACP and was told that the horizontal colored rainbow bars was actually the good video test pattern. It never dawned on me that this was a good test as almost every video test program screen I have come across had some text on them to inform you what you are looking at. The initial Apple Keyboard failures were clearly listed in Basic Information Sheet that USB Hubs and Apple Keyboards would not work with the FireBee. Apple Keyboards have additional USB ports on them which basically makes them hubs. I was in a hurry and didn t pay much attention to the warning.

To Be Continued

Firebee News

Good morning my beloved FireBee crowd,

For the speed and tech nerds below us, there are some interesting news online now. Have a look at http://acp.atari.org

Happy discussion! ;)

Mathias

=~=~=~=

->A-ONE User Group Notes! - Meetings, Shows, and Info!

ACEC 2015 Vintage Computer and Video Game Swap Meet

COMPUTER AND VIDEO GAME FANS:

(The years change, the event doesn’t)

(We regret a number of you will be attending another event scheduled the same day. Next year should be the same weekend in August.)

Reminder: The Atari Computer Enthusiasts of Columbus will yet again be holding their annual vintage computer and video game swap meet, Saturday August 29th 2015. This will be the fourth(?) year at the new location:

Maynard Ave. United Methodist Church
2350 Indianola Ave.
Columbus, Oh.

This church is located on Indianola Ave several blocks south of Hudson St.

The Swap is held in the downstairs of the facility.

Time for the meet is 9:00 a.m. to 3:00 p.m.

Admission is **FREE** for vendors and shoppers. Vendors: please contact Club Prez Charles Brown to reserve tables. Tables are first come, first serve. There is an initial limit of 2 tables per dealer due to space restrictions. However, Charles is willing to listen; at the very least any remaining tables will be distributed if slots are still available just prior to the day. Reserved tables may be also be released for no-shows at 8:30 a.m. the day of the show.

This is not an exclusively Atari show. All vintage and classic computers and video games, systems, accessories, games, and software are welcome.

Charles Brown will create a floor plan page which vendors may use to pick the table(s) that they desire. Please contact Charlie [colonelatari@hotmail.com] for details. (614) 447-9789

Please check our web site often for updates:
http://www.angelfire.com/oh4/acec/acec.html

V/r,
R. Wayne Arenz

=~=~=~=

->In This Week's Gaming Section - Next WoW Expansion Introduces New Class, and More!
  """""""""""""""""""""""""""""""   'Gears of War: Ultimate Edition'!
                                     Windows 10 Is Coming to the Xbox One!
                                     And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""

Next WoW Expansion Introduces New Class, Raises Level Cap, and More

Today during a special video presentation at Gamescom, Blizzard Entertainment announced the sixth expansion for World of Warcraft, called Legion.

The expansion adds a new continent named Broken Isles. It's never been playable in World of Warcraft before, but was referenced in Warcraft 3.

What’s more, Legion raises World of Warcraft’s level cap to 110 and introduces a new class called Demon Hunter (see below for more details on the new character). There are also new dungeons and raids to explore, as well as new artifact weapons and an Honor System.

The new Demon Hunter

Here’s a quick rundown of the key points for Legion, as provided by Blizzard:

New continent: The Broken Isles
New class: Demon Hunter
Artifacts: customizable weapons that grow in power as you do
Class-specific Order Halls and followers
All New Dungeons and Raids
New World Bosses
Level cap raised to 110
Revamped PvP progression system
Improved transmogrification system
Improved social features
Character Boost--immediately raise one character to level 100
Beta starts this year--you can opt in here
New Class: Demon Hunter

The Demon Hunter (no connection to the band of the same name) sounds totally badass. The character can double-jump, and, its creepy-looking wings let it perform gliding attacks to surprise from above. In addition, Demon Hunters are blind, so they rely on "magically augmented sight" to see.

"Dominate your foes as a Demon Hunter, an elven outcast shunned for daring to wield the terrible powers of the Legion," Blizzard said. "Exhibiting superior mobility and a preternatural sense of awareness, Demon Hunters can tap into forbidden powers at times of dire need, metamorphosing into terrifying fel forms. Focus on Havoc to demolish any who stand in your way with fiery demonic attacks, or specialize in Vengeance and go toe to toe with even the most powerful demons, withstanding massive punishment as their attacks fuel your hatred."

New Map: Black Isles

Broken Isles has forests, mountain ranges, and elven cities. There’s quite a bit of danger, too.

"Twisted satyrs, savage drogbar, and cursed Kvaldir prowl the Isles alongside the Legion’s marauding army," Blizzard said. "To overcome these threats, you will claim an Order Hall unique to your character class and lead your followers on a hunt for the Pillars of Creation--the secret to Azeroth’s salvation."

More information about Legion is available on the World of Warcraft website, while Blizzard will hold a developer discussion this coming Sunday, August 9, to talk more about the expansion.

Blizzard has not announced a release date for Legion. Check out some screenshots and concept art images from Legion in the gallery below.

Previous World of Warcraft expansions have included: The Burning Crusade (2007), Wrath of the Lich King (2008), Cataclysm (2010), Mists of Pandaria (2012), and Warlords of Draenor (2014).

With World of Warcraft subscribers sliding, a new expansion could help bring people back. After all, history has shown that new expansions tend to do just that.

’Gears of War: Ultimate Edition’ Includes Full ’Gears’ Collection

Gears of War fans who purchase the Ultimate Edition or Ultimate Edition Bundle for Xbox One will be rewarded with the entire Xbox 360 Gears collection for use on the next-gen console.

Players can tap into the new game on Xbox Live between Aug. 25 and Dec. 31 to gain access to the original three titles, as well as Gears of War: Judgment.

The Ultimate Edition standard and deluxe versions are available now to pre-order for $39.99 and $59.99, respectively.

"In Gears of War: Ultimate Edition, you’ll get the complete remastering of the original game painstakingly reimagined from the ground up with stunning next-gen graphics, recaptured and rebuilt cinematics, new achievements and modernized gameplay for an even better experience," the Xbox Team wrote in a blog post.

The news is part of the Xbox 360-Xbox One backwards compatibility that Microsoft announced at E3. By this fall, 100 Xbox 360 titles will be playable on Xbox One. Select titles were made available to Xbox preview members in June, while everyone else will get a taste in time for the holidays.

So if you already own Gears of War 1, 2, 3, or Gears: Judgment on Xbox 360, save your cash and play them for free on Xbox One. Backward compatibility also works with new features like Game DVR, Snap, and screenshots. Plus, keep previously saved files, add-ons, and achievements, and play with friends via Xbox Live, no matter which Microsoft console you own.

Gears of War: Ultimate Edition also comes with new maps, modes, and missions, early access to the Gears of War 4 multiplayer beta, new achievements, improved haptic feedback, and an additional difficulty level.

"It’s a must-have for every Gears fan and part of the greatest games lineup in Xbox history," the blog said.

The original Gears of War is available today for Xbox One preview program participants. More Xbox news is expected from Microsoft during this week’s gamescom event in Cologne, Germany.

Windows 10 Is Coming to the Xbox One in November

Microsoft first revealed its redesigned Xbox One dashboard back at E3 earlier this year, and now the company is announcing that it will arrive on consoles in November. Powered by Windows 10, the new dashboard

includes features that focus on speed and performance, and a design that’s a lot more simplified.

One of the key new features in the Xbox One dashboard update is Cortana integration. You can say "Hey Cortana, record the last minute and share it to my activity feed" and it will publish a game clip straight away. Likewise, "Hey Cortana, start a party and invite Amanda" will invite a friend into a voice chat all without having to lift your fingers from your controller. Cortana will require the Kinect sensor for audio controls.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Atari Founder Nolan Bushnell on Why Life Is ’A Game’

"I have made so many massive mistakes of ego, I can’t tell you," says Nolan Bushnell leading the way into his crumbling office two floors above a slightly decrepit Los Angeles row of shops.

Inside the offices of Mr Bushnell’s latest start-up - Brainrush - a handful of young men are eagerly banging away on keyboards late on a Saturday afternoon. Ego doesn’t seem to be much in evidence here - at least yet.

While the firm, which was created in 2010, has grand ambitions to transform US education via games, Mr Bushnell remains best-known as the man behind a very different gaming enterprise - Atari.

Now 72, he co-founded Atari - the world’s first video game company back in 1972. It introduced the concept of personal computing, albeit in game form, to millions of households around the world.

Mr Bushnell is also the man who was initially behind Chuck E Cheese’s, the ubiquitous pizza and gaming restaurant chain that has been the site of many a US child’s birthday party (this author included).

But despite all of those early successes - and actually, partly as a result of them - the crumbling office that Mr Bushnell now finds himself in is no deliberately shabby-chic LA decision.

After his breakout success in the late 1970s and early 1980s, Mr Bushnell made several missteps that eventually led to some entrepreneurial failures and financial ruin.

"When I was 35, I was insufferable. I thought I could do no wrong and I got really sloppy," he says.

Now, Mr Bushnell has a habit of referring to his own entrepreneurial journey as if it were a never-developed Atari game.

Mr Bushnell has been a serial entrepreneur from a young age.

He founded a television tube repair business as a teenager that was successful partly because he took advantage of his older customers' penchant to underestimate his technical prowess by undercharging them for his services - but overcharging them for parts.

Later, he worked at amusement parks while putting himself through university to get an electrical engineering degree.

He chalks the creation of Atari up to a bit of good luck: "I was probably the only electrical engineer that understood television, and understood the coin-operated game business [from the amusement park] in 1969," he says.

By combining the popularity of arcade games as well as the nascent personal computer industry, Mr Bushnell and his partner Ted Dabney found success with games such as Pong, Asteroids, and Centipede, which were played, initially, on the Atari 2600 console.

And unlike today's efforts - in which blood and gore in games is both the norm and a scourge - Mr Bushnell said the company believed firmly that it could be successful without resorting to murder.

"We felt that, you could blow up a tank, you could blow up a plane, but we didn't want violence against a human being," he says.

Mr Bushnell also emphasises that the popularity of Atari's games was primarily due to his ability to find and hire talented, creative workers, including one you may have heard of - Steve Jobs.

"I've always valued passionate employees over anything else, and, it turns out that there's a huge percentage of the population that are actually dead - they don't know it, but, in terms of their processes, they're just waiting to be buried," says Mr Bushnell.

But Mr Jobs, like a lot of his earlier employees, had passion and as a result, "was an extremely hard worker".

"He would sleep under his desk at night, and wake up in the morning ready to go," Mr Bushnell remembers.

That unfortunately did come with a bit of a downside: "I think part of the reason [Steve] smelled bad was 'cause he wouldn't necessarily go home every day."

When Mr Bushnell decided to sell Atari to Warner Brothers in 1976 for an estimated $30m (£19m), (a move intended to expand the firm's offerings, but one Mr Bushnell says he now regrets), he carved yet another path, becoming the first of a still-growing list of 20-something Silicon Valley millionaires.

"I want Jobs and [Bill] Gates and [Mark] Zuckerberg and all of these guys to thank me for blazing some of [those trails], because it was much easier once there were several notable successes from [people] in their twenties," he says.
But with that success came hubris.

By the mid 1980s, both Chuck E Cheese and Atari had basically imploded - as had Mr Bushnell's fortunes. Later efforts, including uWink, an entertainment complex featuring food and games as well as robotic

assistants, failed to take off.

But Mr Bushnell remains undeterred, and says he still thinks he has another successful effort in him. He says he’s taken inspiration from his children - some of whom have eschewed university in order to immediately start their own entrepreneurial endeavours.

"How many companies have you started by the time you’re 18? If the answer’s zero, I wouldn’t invest in you," he says of their entrepreneurial verve.

He thinks that biotechnology and virtual reality will be game changers - in addition to his efforts to revolutionise schooling in the US by capitalising on research into cutting edge brain science in order to both personalise education and to make courses more adaptable.

He basically wants to make education as addictive as Atari’s old video games.
"An interesting life can’t be all violins and flowers," he says.

"When you lose a game of chess, you don’t go and jump off a bridge, you reset the pieces and do it again.

"It’s a game!"

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Facebook Rolls Out ’Security Checkup’ Tool to All Desktop Users

Facebook wants you all to have a safe experience on its social network, says Product Manager Melissa Luu-Van who, late last week, revealed how the Menlo Park firm was introducing a new security notification for its web-based users.

After a few months of testing with a limited pool of users, the company has begun rolling out a new "Security Checkup" tool to half of the world’s online population.

If you are one of the estimated 1.5 billion people who log in to the social network at least once a month you will, over the coming weeks, be met with a notification at the top of your desktop newsfeed (Security Checkup for mobile applications is expected to roll out "soon").

A distinctive box, labelled "Stay Secure on Facebook," will urge you to look at three ways you can improve your security on the social site.

While the prompt offers nothing new - its simply a rehashed way of looking at the options under Settings > Security - I would suggest running through it to ensure that your account is as safe as possible.

The three areas covered by the Security Checkup tool are connected devices, login alerts and passwords.

1. Log out or delete unused apps

The first step will present you with a list of previously used browsers and apps that have not been used to connect to the social network for at least a month. By reviewing this list you can ensure that you are only logging in to Facebook from devices and apps that you are still using. You can either log out of all unused apps at once or select specific ones to terminate.

I urge you to go further than that though and cultivate the habit of logging out of anything you aren't using. If you're logged in to something but you aren't using it you're leaving yourself vulnerable to Cross-Site Request Forgery (CSRF) attacks.

2. Get warning of attempted account hijacks

The second part of the checkup will prompt you to enable login alerts if you haven't already done so. When login alerts are enabled, you will receive a notification via your chosen delivery method (the Facebook app, email and/or phone) which will let you know if someone subsequently tries to hijack your account by logging in from a new device or browser.

3. Choose a strong password

Lastly, Facebook uses its new tool to offer up some password tips, such as not reusing login credentials, avoiding the use of names and other common words, and not sharing passwords with anyone else.

This last aspect, while useful, is pretty basic so if you now feel compelled to beef up your password security, the following video is just what you need:

If you haven't received a notification at the top of your newsfeed yet you can still run the Security Checkup right now - it only takes a couple of minutes.

While I think Facebook's decision to encourage its users to consider the security implications of how they use their accounts, as well as previous efforts to educate on the topic of privacy via its lovable blue cartoon privacy dinosaur, are a great step in the right direction, the advice on offer is still pretty basic.

Sure, it's better than nothing, but you may want to do more to protect your account and control your privacy. In which case, you can visit the full set of security and privacy tools via your General Account Settings page.

Or check out our own detailed tips for enhancing your privacy and making your Facebook account safer.

How One School District Is Monitoring Social Media of Students and Teachers

Does your child ever tweet that she "hates" her math teacher?

Does he write that he’s so embarrassed he could jump off a bridge?
Do her posts ever mention being bullied, or does she use them to make fun of other kids?
Are you, as a parent, even aware of everything your kids post?

Even if you aren’t on top of everything your child posts, your kid’s school well might be, given all the social media monitoring software on the market.

If you live in Florida’s Orange County, those kind of posts could mean school officials come looking into whatever’s going on.

That’s because Orange County is one of the latest school districts to start monitoring all of the thousands of social media posts made by both students and teachers.

It’s doing so with a new monitoring software called Snaptrends that monitors social media posts from all accounts in its location.

The school district reportedly paid $14,000 for a one-year Snaptrends license.

That buys the district’s schools the ability to search thousands of posts on sites like Twitter, Facebook and Instagram, hunting for keywords that might indicate trouble.

School officials say that the goal is to flag potential dangers including cyberbullying, suicide and crime.

Joie Cadle of the Orange County School Board told WESH TV that the monitoring will alert school administrators to kids sending potentially serious threats via social media:

If they are sitting in a classroom and they are tweeting because they are mad at their teacher or their girlfriend for whatever reason, and there are some threatening words there, we need to be able to know if it is credible.

It’s not like the posts are private. As Snaptrends’ privacy policy notes, the technology only sifts through public posts.

But opponents of the school’s new snooping effort, which was announced in April, say it’s not the fact that their kids are being surveilled that’s disturbing them.

Rather, it’s the unanswered question of just what, exactly the school district plans to do with the information it collects.

WESH TV quotes Cindy Hamilton, co-founder of Opt Out Orlando:

My privacy issues aren’t with the fact that they’re just out there looking at it, because frankly, with social media it’s not private. But what are they going to do with the information they look at? That’s what we’re concerned about.

When it announced the monitoring, the school district said it will:

[U]se the software to conduct routine monitoring for purposes of prevention or early intervention of potential issues where students or staff could be at risk to themselves or to others.

The company will assist district law enforcement and security personnel in monitoring publicly available social media communications that are relevant to school operations and personnel.

Florida isn’t the only state to turn to monitoring in the face of school shootings, violence and bullying.

As CNN reported last year, the school system in Huntsville, Alabama, hired a retired FBI agent for security work, which included reviewing social media "when a high priority tip is received about an emerging threat to a school, student or staff member," as a school district spokesman said.

As well, the Glendale school district in Los Angeles in 2012 made the controversial decision to pay the firm Geo Listening $40,500 to monitor its students’ social media activity on sites like Twitter, Facebook and Instagram.

The impetus to look into the technology was the suicides of two students. The final decision to pay for the monitoring was made after a pilot program helped administrators step in when yet another student used social media to talk about "ending his life."

The Orange County School District hasn’t detailed how officials will decide what, precisely, to review.

Some technologies might just search social media posts, but others are more akin to tools you might expect to see in the arsenals of government surveillance agencies.

Safe Outlook Corporation’s monitoring software CompuGuardian, for example, gives school administrators not only the ability to search keywords connected to cyberbullying and drug use, but also to delve into students’ search histories to see if they’re researching topics about dangers such as school violence.

CNN quotes Safe Outlook President David Jones:

You can identify a student, and you can jump into their activity logs and see exactly what they’ve typed, exactly where they’ve gone, exactly what they’ve done, and it gives you some history that you can go back to that child and use some disciplinary action.

You can bring in the parent and say, ’Hey, look, this is what your child’s doing. You need to talk to them about it.’

Interestingly enough, and hardly surprising, is the fact that Snaptrends is reportedly also in use by the Central Florida Intelligence Exchange, which is the local law enforcement Fusion Center.

A Fusion Center is a center set up to "analyze information and identify trends to share timely intelligence with federal, state, and local law enforcement including [Department of Homeland Security], which then further shares this information with other members of the Intelligence Community."

As such, it’s not surprising that, just like with the Feds’ propensity to amass vast troves of surveillance data about citizens, so too are opponents pointing to monitoring software’s collection of anything and everything, including both potentially threatening or perfectly innocent

content.

From a post against the surveillance, written by Florida attorney Scott Martin:

Snaptrends is a type of social media scraper/aggregator that collects social media information in mass. The data are scooped up by an automated process without regard to the nature of the content - good, bad, or indifferent.

But what guarantees are there that the social media information collected by the District will be limited to ... benevolent purposes? What policies are in place? Who can access the data? What conclusions are being drawn from the data? Who is drawing those conclusions? What standards are they using in making decisions based on captured data?

All these questions should be answered before any such tool is put in place, Martin says.

I agree.

Right To Be Forgotten Online Could Spread

More than a year ago, in a decision that stunned many American Internet companies, Europe s highest court ruled that search engines were required to grant an unusual right the right to be forgotten. Privacy advocates cheered the decision by the European Court of Justice, which seemed to offer citizens some recourse to what had become a growing menace of modern life: The Internet never forgets, and, in its robotic zeal to collect and organize every scrap of data about everyone, it was beginning to wreak havoc on personal privacy.

Under the ruling, Europeans who felt they were being misrepresented by search results that were no longer accurate or relevant for instance, information about old financial matters, or misdeeds committed as a minor could ask search engines like Google to delink the material. If the request was approved, the information would remain online at the original site, but would no longer come up under certain search engine queries.

Search engines and free speech advocates, calling the ruling vague and overbroad, warned of dire consequences for free expression and the historical record if the right to be forgotten was widely enacted. Now, they say, their fears are being realized.

Recent developments including a French regulator s order that all of Google s sites, including American versions, should grant the right to be forgotten suggest the new right may not end with Europe. Under the banner of privacy, some free-speech watchdogs say, a huge and unwieldy eraser is coming for Google results across the globe even the ones in the United States.

When we re talking about a broadly scoped right to be forgotten that s about altering the historical record or making information that was lawfully public no longer accessible to people, I don t see a way to square that with a fundamental right to access to information, said Emma Llansó, a free expression scholar at the Center for Democracy and Technology, a tech-focused think tank that is funded in part by

corporations, including Google.

Proponents of the right to be forgotten argue such claims are overblown. They point out that the number of removals so far has been relatively small. Since May 2014, Google, by far Europe s most popular search engine, has received requests to forget about a million web links, and has removed about 41 percent of those from certain search results. That s hardly alarming considering the billions of pages online, it s difficult to shed many tears for the mere 400,000 or so that will no longer show up.

Some British news organizations, including the BBC and The Telegraph, have criticized the law for allowing the erasure of hundreds of Google links to news articles, including an excerpt from a mass shooter s rambling manifesto and a slide show entry that called a reality TV star an annoying, unbearable nag. But proponents note that delisted news articles are most likely in the minority of links removed. According to The Guardian, which dug into the source code in a recent Google report to investigate the basis for the removals, more than 99 percent of the links removed were those that showed off private personal details, and were not about public figures or news about serious crimes.

Yet all of this may simply be a prelude to a more expansive, and far more worrisome, adoption of the right to be forgotten. Since Europe s decision last year, several countries in Latin America and Asia have pushed for their own delinking rules, and some of these may elide the protections for free speech outlined in Europe s version of the law. A more troubling prospect for search engines is the potential for the new laws to be applied beyond local jurisdictions.

In response to the original European ruling, search engines began removing links only from European versions of their sites. For instance, if a French citizen requested the removal of links about his bankruptcy proceedings, Google would delete the results from its European sites like the French Google.fr and the German Google.de but not from Google.com, which the company considers its American site.

The overwhelming majority of Google searches in Europe take place on country-specific sites, but because Google.com is still accessible to any European, the French data protection authority, known by its French acronym the CNIL, has ordered Google to remove links from its database entirely, across all locations.

Google has so far refused, and the dispute is likely to end up in European courts. If the French understanding of the law prevails, the regulation could have far-reaching, even chaotic, effects.

 France is asking for Google to do something here in the U.S. that if the U.S. government asked for, it would be against the First Amendment, said Jonathan L. Zittrain, who teaches digital law at Harvard Law School. He pointed out that, if enacted, the French regulator s order would prevent Americans using an American search engine from seeing content that is legal in the United States. That is extremely worrisome to me.

If other countries that have established a right to be forgotten also push for global adoption, Google says it might need to remove links everywhere to satisfy regulators. We believe that no one country should have the authority to control what content someone in a second country can access, Peter Fleischer, Google s global privacy counsel, wrote in a blog post last week.

A host of free speech advocates have sided with Google. If we re asking Google to comply in every version of Google worldwide, it becomes very hard to say where we want Google to draw the line, said Jimmy Wales, the founder of the online encyclopedia Wikipedia, which has counted about 100 requests for links to its site to be removed from search engines in Europe. It s a race to the bottom. Governments all around the world will immediately say, Great, we ll ask for things to be deleted worldwide.

Representatives for the CNIL, which has two months to answer Google s refusal to adopt a worldwide takedown, declined to discuss the case until it devised a formal response. But legal experts in France said the French demand was likely to be upheld, because the original 1995 law on which the right to be forgotten is founded has no territorial restrictions.

Proponents of the law also reacted skeptically to the claim that the right to be forgotten would be used by other countries to force content restrictions beyond those involving privacy.

 That s nonsense, said Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy advocacy group. He argued there were ways to limit access to private information that would not conflict with free speech, and he noted that Google already had a process for global removal of some identifiable private information, like bank account numbers, social security numbers and sexually explicit images uploaded without the subject s consent (known as revenge porn.).

 A global implementation of the fundamental right to privacy on the Internet would be a spectacular achievement, said Mr. Rotenberg. For users, it would be a fantastic development.

Mr. Zittrain, of Harvard, pointed out that Google also removes content globally to abide by copyright law. When Google receives a takedown notice for linking to infringing content, it removes those links from all of its sites across the world. Couldn t it do the same for private information?

The trouble with comparing copyright law to privacy, though, is that the United States and Europe broadly agree on what constitutes copyrighted content, but private information is far more nebulous.

In an interview last year, Larry Page, Google s chief executive, told me that he found the right to be forgotten ruling impractical because it forced Google to decide what constituted private information and what did not. You guys are now in charge of editing what s out there in the world, he said, describing the court s guidance to Google. In the past that s not a responsibility we felt we had.

Is an article about a British reality TV star about a private person, or is it about a public figure that you and I should be able to search for?

That s hard to answer   but a French regulator may soon decide for you, regardless.

Firefox Users, Here’s A Security Flaw You’ll Need To Fix

Another day, another security flaw - this one affecting Mozilla’s Web browser, Firefox. But this one is easy enough for you to fix.

On Thursday, Mozilla revealed a vulnerability in its browser that was discovered by a Firefox user. An ad on an unnamed news site in Russia was able to tap into the vulnerability to upload certain files from a user's computer to a server apparently based in the Ukraine. Exploiting Firefox's PDF Viewer and its use of the widespread JavaScript code, the hack seems to capture only "developer focused" files - think FTP (file transfer protocol) - at least in Windows. Your personal files and data aren't caught in the attack, but the hack is still alarming.

Has the world grown weary of security hacks and exploits at this point? Each day, those who browse the Web or use Windows or Adobe Flash or numerous other products seem to face yet another security worry. Even the Mac OS, which has long held a reputation as being secure, isn't immune. Software is imperfect, and hackers are always going to find a way to exploit certain weaknesses. So what do we do? Protect our computers with security software. Be careful of where we go and what we do on the Internet. Hope that vendors quickly find and fix the vulnerabilities. And Mozilla had done just that.

Released on Thursday, the latest version of Firefox - version 39.0.3 - contains a fix for the security hole. Mozilla is urging all Firefox users to upgrade to this latest version.

To update Firefox to the latest version, click on the Help menu from the Menu Bar or the Firefox button in the upper left corner. Then click on the setting for About Firefox. If you don't already have the latest version, you should see a button that reads "Update to 39.0.3." Click on that button, and Firefox will automatically update itself to the new, secure version, and then prompt you to restart it.

The vulnerability affects both Windows and Linux. It does not affect the Firefox mobile app for Android as that program does not contain the PDF Viewer. It has not affected Macs as of yet, but Mozilla said that Apple's OS X would not be impregnable if someone were to target it. People who use software that blocks ads on the Web may have been protected from the security flaw, but that depends on the specific program and filters in place.

Mozilla expressed surprise at the types of files that were targeted.

"The files it was looking for were surprisingly developer focused for an exploit launched on a general audience news site, though of course we don't know where else the malicious ad might have been deployed," Mozilla security lead Daniel Veditz said in Thursday's security blog.

Veditz added this sobering thought: "The exploit leaves no trace it has been run on the local machine."

Why You Shouldn't Freak Out About This Week's Scary-sounding Mac Exploits

One set of researchers explains how a modification to your Macintosh s boot-up firmware can persist undetectably and spread through peripherals to other computers. Another researcher s work from a month ago is found in the wild, installing adware through a hidden escalation in user privileges. Both sound terrible, but neither is quite what it seems.

A month ago, a security researcher who has found previous flaws in iOS, Stefan Esser, documented a problem in OS X about which he didn t warn Apple in advance. Starting in Yosemite, OS X allowed software to log errors to an arbitrary file. Esser discovered that this could be used maliciously to write to files that only a root user should be able to. He took that weakness to demonstrate how one might escalate privileges, allowing a regular user without administrator or root access to run any software he or she wishes.

I didn t cover this back when it was announced for three reasons: First, I d prefer to not give attention to researchers who opt out of following the industry standard of revealing zero-day (immediately exploitable and unpatched) security flaws to the company or organization responsible for updating the software. This is unavoidable when it s severe enough, because people need to be informed about risks and mitigations.

Revealing zero-days injures end users at the expense of making a point about one s frustration with a firm, or for those who simply don t care, it demonstrates a lack of ethics about one s actions. If the motivation is disgust with Apple or another company s responsiveness to security flaws, I ve seen other researchers just as effectively make the point by disclosing 60 days or several months after an initial flaw goes unpatched if the software maker is truly avoiding the problem. This was the case with NetUSB in May, a flaw that affect millions of routers, and which only some affect companies chose to act on.

Don t install software from any old place on the Internet.

My second reason: To exploit this flaw, one has to have a way to run software as a local user. This requires a separate zero-day that acts as a trigger, or relying on the naivetØ of a user who installs software from random sites not from Apple or known third-party developers.

The flaw isn t insignificant: it s truly dangerous and severe. But because exploiting it almost certainly requires users to engage in behavior that is already extremely risky, a privilege escalation isn t per se more severe than them installing software from download sites, via torrents, or through other untrusted sources and using an administrator password when prompted.

Third, I assumed it was the sort of thing that would be quickly patched, because it s such a trivial error, rather than a deeply nested part of OS X that would require new plumbing. In fact, Apple had received a report well before Esser s disclosure, and was already working on the problem.

Apple tells me that the latest developer beta of 10.10.5 contains the fix.

Unfortunately, before Apple made the fix, malware was discovered in the wild this week in an adware installer that s an installer for legitimate software that also adds adware with affiliate programs. These malicious installers don t hack a computer, so much as provide a revenue stream for those who release them.

Apple tells me that the latest developer beta of 10.10.5 contains the fix, which Esser confirmed a few days ago; OS X 10.11 El Capitan approaches this particular feature differently, and didn t suffer from the flaw. The date for 10.10.5 s release wasn t disclosed.

Did Apple patch that flaw yet? Can I stop hiding now?

The adware installer found in the wild that exploits this flaw used a signed developed certificate, which Apple has revoked. Apple has further added a signature to XProtect, its anti-malware database, which should be updated by this writing to prevent the original installer and ones using similar code from running.

Esser isn t wrong to be frustrated at the uneven pace by which Apple fixes system flaws. The company is sometimes lightning fast, and sometimes lets issues lag for months or longer. But it s hard to support this form of disclosure unless one is certain Apple is ignoring the problem because Apple certainly isn t harmed in any substantive way by being punished with no advance warning. Users are.

Also this week, researchers said they had found vulnerabilities in Apple s bootloader software, EFI (Extensible Firmware Interface), different forms of which are widely used for all modern personal computers, whether they run OS X, Windows, or a Unix variant. EFI resides in firmware, and launches when a computer is powered up or restarted, initializing hardware and loading the operating system. (In the not-that-long-ago days, the PC world used BIOS, for basic input/output system, which EFI replaces.)

One of the two researchers demonstrated Thunderstrike earlier this year, a way of modifying EFI firmware through Thunderbolt hardware, which can contain the equivalent of firmware extensions via built-in option ROMs. Option ROMs are designed to extend EFI to support specific hardware features hence the term extensible in EFI s name. Not enough checking was done to prevent malicious software from running and patching EFI. The 10.10.2 update closed the hole that allowed Thunderstrike to work, but researcher Trammell Hudson said months ago that other vulnerabilities remain if one can gain physical access to a Mac.

He and Xeno Kovah plan to show a demonstration of Thunderstrike 2 this week in Las Vegas at the Def Con computer security conference. This variant takes a different approach to the same sort of attack, and more worryingly can spread as a worm among infected devices. However, it still requires several steps to accomplish its task.

The worm has to be delivered, which requires either physical access (through a malicious or innocent party with an infected device) or via a separate exploit to install or a way to convince a user, as with the escalation flaw discussed above. Once the malware is loaded, the malware copies itself to any other attached Thunderbolt device s option ROMs, including peripherals as simple as a Thunderbolt gigabit ethernet adapter.

"Any worms in here? Do not want."

When a Mac is next restarted with an infected option ROM, the malicious software is added to its EFI firmware, providing a new vector. Any infected peripheral that s shifted from that Mac to another spreads the malware. While Apple checks for the integrity of firmware updates before they re installed, it doesn t otherwise check option ROMs or EFI firmware at other points.

Apple says that as of 10.10.4 (released in June), the demonstration that Kovah and Hudson plan to show will not work, as they ve patched the vector used. Via email, Hudson pointed me to an update on his site on Wednesday that acknowledges one avenue of attack was shut down, but

others remain, including using option ROMs to spread their worm. Apple says it s investigating these other reported weaknesses.

Apple says that as of 10.10.4 (released in June), the demonstration that the researchers plan to show will not work, as they ve patched the vector used.
But it s crystal clear from the researchers work that more fundamental changes need to be made to ensure that holes aren t just plugged. Two months ago, yet another EFI flaw was found and quickly patched by Apple as part of the 10.10.4 release.

A rethink of firmware integrity is needed, and not just by Apple. The two researchers more broadly found problems across the industry in EFI bootloaders. As I noted two months ago, peripheral firmware appears to already have been exploited by national-security agencies, and would thus also be a likely target for criminals as well. This kind of attack isn t theoretical nor just a good demo. Computer vendors need to step up to the new state of firmware risks.

No, Your Mac Isn t Immune to Malware

Mac users have always been a little bit smug when it comes to cybersecurity. Apple even brought up its product’s resistance to viruses and malware in the famous line of Mac vs. PC commercials from the mid 2000s. "You’re lucky you don’t have to deal with this stuff, Mac," John Hodgman’s biohazard suit-clad PC tells a Mac played by Justin Long.

But a new worm could end the myth of Max invincibility. The hack developed by researchers Xeno Kovah and Trammell Hudson can attack the firmware of Macs and all top PC makers, according to Wired. This malware was created not by hackers but by the researchers to show that it could be done.

Firmware is code that starts running as soon as a computer is turned on and starts to load its operating system. That makes the malware particularly hard to detect and fight: Even reinstalling an operating system could leave the worm nesting in the firmware, untouched.

The worm relies on a collection of firmware vulnerabilities that the researchers found in both PCs and Macs. More about the research will be revealed at a cybersecurity conference in Las Vegas later this week, according to Wired.

Wired also reported that the researchers notified Apple of the firmware vulnerabilities that affect Macs and that the company has patched some, but not all, of the issues. The worm will not work with the latest version of Apple software, according to a person with knowledge of the issue.

Apple declined to immediately comment on the report.

But this isn’t the first time security vulnerabilities have affected Apple users. Last year Apple admitted that its version of SSL, the encryption that protects much of online communications, had a flaw that could allow hackers to intercept and modify traffic thought to be secure. The problem affected both its mobile operating system iOS and its laptop and desktop suite OS X. And in earlier years, some OS X users fell prey to a Trojan

malware known as Flashback.

What s Safer From Hackers: A PC Or A Mac?

Mac vs. PC. (Images by Thinkstock/Apple/Microsoft, modified by Yahoo Tech)
Apple s vaunted reputation for safety and security has taken some hits recently. Just this week came news of DYLD_PRINT_TO_FILE a bug in Apple s OS X operating system that has allowed a malicious program to take complete control of Macs. Apple has known of the flaw for a few weeks but hasn t gotten out a patch yet. Then there were reports of a vulnerability in the Mac s firmware that could allow infections to pass among Macs via Thunderbolt accessories.

This isn t to pick on Apple too much. Microsoft Windows has obviously suffered from regular security flaws over the years. But Apple is the one that s historically claimed to have the safer, more secure platform. Is that claim true?

Before you compare OS X and Windows, you have to remember that security is about more than just the operating system: The biggest threats can run on both platforms. Just last month, for example, researchers learned of a big flaw in Adobe Flash that would allow an infection from a website to take complete control of any computer, Windows or Mac.

So we decided to take a look at the big picture, comparing Windows and OS X on overall hackability. Overall, Apple OS X is still a bit more secure than Microsoft Windows, but the gap keeps narrowing. Ultimately, the safest operating system is the one run by an informed user who knows how to keep it up to date, knows what to install, and knows what to remove.

When it comes to security flaws, Windows and OS X are now about tied, says Morey Haber, VP of technology at corporate security software maker BeyondTrust. Combing through security alerts and updates, Haber calculated that for 2014, Windows had 142 vulnerabilities while OS X had 147.

But operating system vulnerabilities accounted for only 13 percent of all reported computer security issues in 2014, according to Haber; software that runs on both systems accounted for 80 percent. Most hackers aren t even targeting the operating system anymore, says Haber. They go after software like Adobe Flash, a platform for Web-based videos and games (more about Flash later).

Macs biggest security asset is basic economics. I ll stick on my Mac over my Windows box, and the simple reason is statistics, said Haber. Hackers are targeting Windows because there are more devices out there.

The winner here: OS X?Macs are a scoche safer simply because they are less likely to be targeted in cyberattacks.

Your Web browser is not only the front door to all the charms of the Internet, it s also a backdoor for attackers. A particularly nasty attack method is called a drive-by download: Simply visiting a website running malicious code can infect your computer. I ve seen upwards of 50 different exploits in the one link, says Chase Cunningham, threat

intelligence lead at security firm FireHost. It just tries everything it can. But it gets worse. You can get infected by visiting a perfectly legit site with booby-trapped animated ads that slip into the automated networks that place ads on Web pages.

In 2014, Internet Explorer was found to have 220 vulnerabilities rated as high, Chrome had 86, and Firefox had 57, according to Haber. He can t get an exact count of flaws in the Apple Safari browser, says Haber, because Apple generally doesn t provide detailed descriptions of vulnerabilities and fixes, as other software makers do.

Other major dangers are the powerful plugin programs that extend the functions of the browser. In 2014, 65 security vulnerabilities were discovered in Adobe Flash; Oracle s Java plugin had 50. Many attacks are on older versions of plugins because they generally don t update automatically or prod users as aggressively to install new versions.

 All of the operating system [and] the browser vendors realize that plugins are problematic, said Haber. [They] are a bad user experience, and [companies] are turning them off.

OS X has been more active in choking off the vulnerable plugin problem. Apple stopped installing Flash on its computers in 2010 (although Mac owners can manually install it). You can often get by without Flash, as many sites are replacing it with alternatives built into the HTML 5 Web programming standard. Amazon Instant Video, Netflix, YouTube and Vimeo, for instance, have already switched over or are switching over.

Java can be installed both as a standalone app and as a browser plugin. Apple stopped preinstalling Java with OS X Lion (10.7) back in 2011. In 2012, it issued an update that removed the Java plugin from all installed Web browsers. (Mac owners can install Java on their own.) Java has been falling out of favor for years. I don t have it enabled in any of my browsers, said Guillaume Ross, senior consultant at security company Rapid7. I m trying to remember the last time I needed Java.

Microsoft has removed plugins from its successor to Internet Explorer, called Microsoft Edge, which comes with Windows 10. (Though a future version of Edge will bring back some kind of plugin compatibility, Microsoft has said.)

The winner here: OS X?Both Apple and Microsoft are pulling out browser vulnerabilities, but Apple has been working on it longer.

Other programs are less likely targets for hackers, but they may have security flaws. Any application that you install will increase your attack surface, said Ross.

Apple and Microsoft have responded by creating app stores. Not only have they evaluated the apps to insure that they are genuine, but they also require security measures called sandboxing, which limit a program s access to the operating system and other applications. Versions of the same program offered as a download from, say, the vendor s website may not have sandboxing measures, however. I would definitely pick the app store application when there are two, said Ross.

If a program isn t in an app store, the next line of defense is to check if it s digitally signed by the software maker. By default, OS X allows only apps from the App Store or those that have been signed by known software makers.

The winner here: OS X! Apple s automated security for programs protects users better.

Apple s security edge is based largely on what the operating system does by default. But you can do a lot to make either system much safer.

Install those updates your computer keeps nagging you about, or enable auto updates. Microsoft currently provides security updates for Windows Vista, 7, 8/8.1 and 10 (there is no Windows 9). Apple tends to support the latest two or three versions of OS X. Right now, that s 10.8 Mountain Lion, 10.9 Mavericks and 10.10 Yosemite.

As earlier explained, Flash has been on the wane for years. Whether you have a Mac or Windows computer, you can easily flush it from your system or keep it disabled until you need it.

Java is of even less use nowadays. Oracle offers instructions for uninstalling Java from Windows computers and more-technical instructions for removing Java from a Mac.

Get programs from the app stores in Windows and OS X whenever you can. If a program isn t in the app store, make sure it s genuine by going to the vendor s own website instead of some generic download site (or pirate site).

In Windows, check the digital signature: Right-click the program installer you have downloaded and click Properties to see if the name on the signature is the same as the maker of the software. On a Mac, go to the Security and Privacy preferences; under Allow apps downloaded from: click the button labeled Mac App Store and identified developers.

If you do download a bogus app, encounter a website that exploits a Flash or Java vulnerability, or forget to update your OS, security software acts as a safety net. This is a competitive product category, so most packages do a good job, and many are free for personal use. For an in-depth comparison, check the latest rankings on AV-Test.org.

The overall takeaway is this: All computers can be hacked. Apple, by shedding default plugins and blocking automatic installation of unsigned third-party apps on Macs, has traditionally made it easier for average folks to keep themselves safe. But on the flip side, Windows, running on almost 90 percent of all computers operating today, has always been a juicier target for virus and malware makers. Most attacks now work equally well on both operating systems. So staying safe isn t so much a matter of what computer you buy, but rather how well you understand and avoid the security pitfalls on it.

=~=~=~=